A 9-Dimension Grid for the Evaluation of Central Bank Digital Currencies

José Parra Moyano	Arthur Macherel	Adrien Treccani
University of Zurich	University of Zurich	EPFL

Abstract:

Blockchain technology offers new opportunities for the development of central bank digital currencies (CBDCs). Although discussion on the matter is still in its early stages, researchers and practitioners have proposed possible frameworks via which to explore the potential of this new form of money for central banks and governments. Since blockchain technology is very broad, central banks can conceive of many different blockchain types to sustain CBDC, and the decisions taken by a central bank at a technical level determine the economic possibilities of the resulting monetary system. In other words, the technical attributes of a blockchain have crucial implications for the monetary system that such a blockchain might sustain. In this article, we propose a grid that identifies nine fundamental technical dimensions to be assessed by central banks when establishing a digital currency system based on blockchain technology, and that analyzes the different implications for the central bank as it moves through each of the identified dimensions. Our objective is to offer this grid as a tool to aid in the structured, conceptual, and technical development of national currencies based on blockchain. By way of illustration, we use the grid to analyze three practical scenarios that significantly vary in their implications for the monetary system.

Keywords: Blockchain, Distributed Ledger Technology, CBDC

1 Introduction

Distributed ledger technology (DLT) in general and blockchain technology in particular have attracted significant attention over recent years. Several commercial banks, IT companies, and financial intermediaries are investing considerable resources to develop applications based on these technologies. One of the applications of blockchain technology discussed in recent years is the generation of central bank digital currencies (CBDCs). Barrader and Kumhof (2016) state that the macroeconomic consequences of issuing CBDC could include a permanent rise in GDP of as much as 3 percent caused by reductions in real interest rates, distortionary taxes, and monetary transaction costs. We postulate that CBDCs will eventually exist, or at least that central banks (CBs) will explore the development of CBDCs in many possible forms. Indeed, the People's Bank of China and Russian state-owned Sberbank are both exploring these possibilities today and are developing proofs of concept in this direction.

We suggest a structured 9-dimension grid that CBs can use to evaluate the various options with regard to implementing CBDC and that works as a structured, conceptual framework that helps CBs to compare the different options they have when it comes to the development of CBDC. The grid addresses nine different questions that a CB has to answer when considering the development of CBDC and the answers combine to lead to different CBDC scenarios. While theoretically many such scenarios are possible, only a limited number are viable given the current context in which CBs operate. Among these workable scenarios there is, however, enough variability to allow CBs to develop CBDC systems that significantly differ from one another.

We carried out an extensive review of the literature for each of the nine dimensions that make up the grid. We address topics such as the permissioned degree and the consensus protocol used by the CB to maintain the blockchain and hence the system, the right to mint money and transact

that different users of the system might have, the privacy of the transactions, and the scalability of the whole system. For each level we provide a short rationale of blockchain technology in level-specific terms. That done, we analyze the implications of the decision taken with regard to each dimension and describe some possible scenarios that might arise from the application of the grid. Our aim is to set the foundation for a structured comparison of different blockchain-based CBDCs.

In Section 2 we describe the current cash cycle from the perspective of money creation and circulation in order to have a benchmark for any new proposed system. Section 3 provides a short introduction to blockchain technology. In Section 4 we explain how our approach uses design science research. We introduce the nine dimensions that define a blockchain and the implications of each of these dimensions for a CBDC system in Section 5. In Section 6 we compare three scenarios that result from different combinations of the dimensions described in Section 5. In Section 7 we conclude.

2 The cash cycle today

Anyone who wishes to propose a credible CBDC scenario must possess a solid understanding of the current money cycle. In this section we provide a brief overview of the way money is created by central and commercial banks, of how transactions are carried out in the financial system by the system's participants, and of different monetary policy strategies.

2.1 Money creation

Money is a special type of IOU ("I owe you"), trusted and accepted by all agents in an economy (McLeay et al., 2014b). Money is defined by three characteristics (Clews et al., 2010)—namely, the ability to store value, serve as a medium of exchange, and serve as a unit of account. The ability to store value is the ability to transfer purchasing power to a later date. A medium of

exchange is a commonly accepted support used to make payments. A unit of account is the metric used to define the value of any item that can be sold. Hence, money is a specific type of financial asset and "[b]ecause financial assets are claims on someone else in the economy, they are also financial liabilities – one person's financial asset is always someone else's debt" (McLeay et al., 2014b). In the case of national fiat currencies, the respective CB is the ultimate bearer of all fiat liabilities.

Open market operation is the main tool used by CBs to create money in an economy. This operation consists in buying or selling securities, such as government bonds, in the open market. Purchasing securities is equivalent to adding money to the system, while selling them corresponds to removing money (Federal Reserve System, 2017). Commercial banks and financial institutions that meet specific criteria are usually the counterparties in these operations. This simplifies but also limits the diffusion of money through the system. The CB can be compared to the money's wholesaler, while commercial banks are its retailers. Hence, other companies, households, and individuals are only able to access money through these providers. There are two types of money in this system, broad and base. Broad money is composed of all fiat currency and commercial banks' liabilities to agents other than the CB, also known as deposits. Base money includes all fiat currency plus liabilities of the CB with regard to commercial banks " (McLeay et al., 2014b). Fiat currency usually transits through commercial banks before reaching "end users"[1]. Hence, commercial banks are significant money creators in modern economies " (McLeay et al., 2014b).

One of the main functions of commercial banks is to collect deposits. Commercial banks lend these deposits only if they exceed the sum of their reserves plus their currency holdings " (McLeay

[1] Throughout this paper we refer to the users of CBDCs, in the broadest sense of "users"—that is to say, the general public, as "end users".

et al., 2014b). These new loans, to a certain extent, create new deposits, which the banks then use for further lending. This mechanism, also known as fractional banking, multiplies the amount of liabilities and therefore the value of *broad* money.

"Monetary policy is the ultimate constraint on money creation" (McLeay et al., 2014b). The primary objective of monetary policy is to maintain price stability by using different policy instruments (European Central Bank, 2011a). The transmission of monetary policy is characterized by changes in official interest rates (European Central Bank, 2011b). There is usually a lag between a change and the effects on prices because the change passes through multiple layers, including commercial banks.

2.2. Transactions

The Committee on Payment and Settlement Systems (2003) has defined payment as "the discharge of an obligation by a transfer of funds and a transfer of securities that have become irrevocable and unconditional". In this context, money is a means of transferring value to other agents. The simplest type of money transmission is the cash transaction. Debt settlement is direct and straightforward in the form of a physical transfer of coins and banknotes from a payer to a payee. The system becomes more complex when it comes to digital money. As such money is dematerialized, a triangular payment structure with an intermediary is usually required (Rossi, 2004). The multiple agents taking part in a transaction must interact and agree on a framework that will ensure a secure and irrevocable transfer of value for debt settlement.

Payments systems are composed of multiple instruments and procedures designed by banks (Rambure and Nacamuli, 2008). Instruments are tools used for transactions, and include credit or debit cards, checks, and ATMs. Procedures are series of actions used to generate transactions.

An example of a procedure is the balance query sent to an agent's bank when he or she initiates a payment at an electronic point of sale (Brown, 2014). If the query returns a sufficient balance the transaction can be processed further, otherwise it is declined. When using such systems to make transactions, agents accept the conditions established by the multiple institutions they are dealing with. Most systems operate within a legal framework set by state regulatory agencies—frameworks that ensure the agent of a certain level of security while using these systems. A transaction between clients of the same bank is the most straightforward case in digital payment systems. The system becomes more complex, however, when the transacting agents do not hold accounts at the same institution.

In the current financial system there are three ways of executing a transaction between two agents that hold accounts at different banks—namely, correspondent banking, deferred net settlement (DNS) systems, and real-time gross settlement (RTGS) systems (Brown, 2013). Further, there are three criteria with which to assess the efficiency of each option: execution time, risk, and cost (Rambure and Nacamuli, 2008).

3 Blockchain technology

DLT concepts date back to 1990 with proposals for distributed accounting systems (Attewell, 1992). The development of functioning systems picked up only recently, however, with Nakamoto's (2008) proposal for a distributed currency registered in a series of consecutive blocks, commonly called a blockchain. This significant finding soon led to numerous modified versions of blockchain designed for specific needs, resulting in the creation of many alternative coins. We refer the reader to the various papers available (Cachin, 2016; ASTRI, 2016; Pilkington, 2015; Swan, 2015; Nakamoto, 2008) for an in-depth explanation regarding this topic.

Conventional ledger systems are usually managed and updated by specific agents such as banks or financial intermediaries—agents that need to be trusted by the systems' users. But a blockchain is a peer-to-peer distributed ledger technology and "a distributed ledger system that is collectively maintained by all the participants of that system" (ASTRI, 2016). Blockchain's terminology defines two layers: the fabric and the application layer. According to Glaser (2017), "whoever develops and maintains the fabric layer is in ultimate control of the whole system's functioning". An agent with full control of the fabric layer is, technically speaking, the owner of the system. In contrast, the application layer can be developed by anyone and bound to the fabric layer. "The code itself is then under control of the participant who deployed the piece of code" (Glaser, 2017). Digital wallets are a good example of applications. A simple analogy via which to understand how DLT functions is to think of a public room where everyone is entitled to an amount in virtual tokens that they can exchange. These tokens cannot be physically transferred, but like digital money their ownership can be recorded in a blockchain. Participating in the recording system can result in a reward in the form of new tokens and transaction fees.

The formal functioning of a "permissionless" blockchain assumes that any node can join and participate in the network and that strictly more than 50 percent of nodes are honest (Nakamoto, 2008). Further, nodes are assumed to be rational and therefore always prefer the outcome with the highest expected return. As an incentive to verify and validate transactions, the protocol awards the node presenting a valid block a specific amount of money in new tokens. Without coordination this would result in numerous nodes continuously presenting blocks. Hence, a protocol with regard to the addition of blocks to the blockchain is implemented in the system. Proof-of-work (PoW), proof-of-stake (PoS), and proof-of-authority (PoA) are the most common protocols used in blockchains today.

The concept of PoW relies on the fact that certain data is difficult (costly and time-consuming) to generate but easy to verify. This concept introduces competition among “miners” (see next paragraph) and sets the incentives that enable the system to work, such that the most efficient node—the node that generates the data in the fastest and most efficient way—is enabled to generate the next block and receives the abovementioned reward. The concept of PoS relies on a random selection on grounds of wealth or age (i.e., the stake) to define which node will be enabled to create the next block and thus will receive the reward. PoW is computationally much more intensive than PoS. PoA is an alternative to PoS or PoW; it can be used for private chain setups because it uses a set of arbitrarily defined “authorities” that select the creator of each new block.

A node that validates transactions is commonly referred to as a miner. Mining is the activity of solving cryptographic puzzles that are generated by the protocol. These puzzles can only be solved using computational force. Hence, the time required, equivalent to hardware and electricity costs for a node, is a decreasing function of the computational power used. The protocol adjusts the difficulty of the puzzle for each new block to the computational power available on the network. It ensures that solutions are found, on average, at fixed intervals of time. For example, a cryptographic puzzle generated is solved every 10 minutes on the Bitcoin network (Nakamoto, 2008). The successful node then presents the PoW, proving it has solved the puzzle and has the right to broadcast its block to the network and add it to the blockchain. Additionally, the node receives transaction fees and receives a reward in the form of coins. All other nodes easily check the validity of the transactions of the new block. If consensus with regard to the new block’s validity is reached among a majority of nodes, the block is accepted and added to the blockchain and the network goes to the next PoW. As a malicious node can add a block containing fraudulent transactions, a solution is required to avoid successful nodes from broadcasting such blocks.

If other nodes checking a block's validity notice fraudulent transactions, they keep mining the PoW of that block. The puzzle is eventually solved by another node, which broadcasts its block, thus creating a soft fork in the blockchain. Assuming the second block is honest, there is competition between the two. All nodes start mining the next cryptographic puzzle. Given the protocol specifications, there is a negligible probability that the same node can solve subsequent puzzles and add blocks (Nakamoto, 2008). Hence, the next successful node can choose to broadcast and add its block after either of the two previous blocks. Given the higher proportion of honest nodes, the expected growth of the honest fork is greater. As the shortest chain is disregarded and collapses, all rewards are lost for the nodes that added blocks to it. This implies that building on a fraudulent block carries with it a high opportunity cost, even for other malicious nodes. The protocol thus ensures that nodes have the incentive to behave honestly. If they do not, they will have invested costly computational time but will not be rewarded for doing so. This mechanism depends on the specifications of the blockchain.

The distributed copy of the blockchain ensures that the chain is tamper proof. It is not possible for a node to overwrite, add, or delete any entry in the blockchain without other nodes noticing it. Hence, "DLT is built upon a series of networks of databases that allow participants to create, disseminate and store information in an efficient and secure manner. These networks of databases can operate smoothly and securely without the need for any central party or central administrator that every participant knows and trusts" (ASTRI, 2016).

4 Research design

Gregor (2006) defines a taxonomy of theory types in information systems research to classify information systems theories with respect to the manner in which four central goals are addressed: analysis, explanation, prediction, and prescription. Specifically, he focuses on five

interrelated types of theory: (1) theory for analyzing, (2) theory for explaining, (3) theory for predicting, (4) theory for explaining and predicting, and (5) theory for design and action. The theory for design and action explains how to develop a new system and gives explicit prescriptions (e.g., methods, techniques, principles of form and function) for constructing an artifact. We frame our research within this theory for design and action because our aim is to give specific guidance to CBs on how to construct a monetary system based on blockchain technology.

Hevner et al. (2004), March and Smith (1995), and Gregor (2006) consider that contributions to knowledge within the theory for design and action can be measured according to the utility that they bring to a community of users, the novelty of the artifact resulting from the research, and the persuasiveness of claims that this artifact is effective. Gregor (2006) further states that models and methods can be evaluated with regard to their completeness, simplicity, consistency, and ease of use, and to the quality of results obtained.

We followed four steps in developing our theory. First, we analyzed the logic of the existing monetary system to summarize and describe the current definition, creation, and transmission of money. Second, we described the blockchain technology and the different dimensions that compose a blockchain and that can be arbitrarily set by the designer of a blockchain. Third, we put the logic of the existing monetary system described in step one together with the dimensions that can be arbitrarily set by the designer of a blockchain (step two), thus defining the possible scope of systems that enable the creation of CBDC. Fourth, we analyzed three of the resulting scenarios out of the whole space derived in the third step, exemplarily showing the different implications of each design. Our theory can be categorized as “theory for analyzing” which corresponds to Gregor’s (2006) first type of theory. Following Hevner et al. (2004), March and Smith (1995), and Gregor (2006) we should evaluate our theory according to it the utility for the community of users, the novelty of the resulting artifact, and the persuasiveness of the artifacts’

claims. As we will prove in section 6, the grid resulting from this theory is useful for the community of researchers and economists exploring CBDCs, since it can be applied to compare different CBDC-scenarios in a structured manner, which serves as a solid basis to evaluate the implications of technical innovations for the users' needs. The result of this paper comes along with a high level of novelty, since it yields the ground for the comparison of scenarios that have not yet been developed –no central bank is yet using blockchain technology as the foundation for its monetary system. Finally, the persuasiveness of the results claims can only be assessed by the users of grid, once this one has been applied. Nevertheless, since the grid can incorporate further dimensions if required, it is easily adaptable to address criticism of the users and incorporate future dimensions that might arise when the technology keeps evolving.

5 A cash cycle based on blockchain

Blockchain technology is a modular system with features that can be adapted to users' needs. There has been a remarkable development of DLT and blockchain solutions over recent years. Beyond the qualities that we discuss in Section 2, we assume that a set of requirements will be defined by the CB before designing a blockchain-based system for the emission of CBDC. Here we propose three assumptions that we consider valid whenever a CB embarks on the design of such a system.

First, the CB retains direct or indirect control over the blockchain and its fabric layer. It is not realistic for a CB to have no control over the underlying system it uses for emitting its national currency. In the context of this paper, full control or control shared with a supranational entity (such as the Bank for International Settlements (BIS)) are acceptable. Second, the CB has to be able to identify at any time any agents or transaction in the system. This does not imply that the CB is informed about everything at all times but that the necessary information must be available

to it. Numerous DLT systems offer highly secure anonymity using cryptographic solutions. Given anti-money-laundering (AML) regulations, know-your-customer (KYC) procedures, and tax laws, it is not realistic for a CB to create a CBDC system in which users can store and transfer value in a completely anonymous manner. Third, the CB ensures privacy on the network. In a similar way to RTGS, the CB does not disclose CBDC transaction details. Doing so might result in distrust from users.

In the following subsections we introduce the nine dimensions that compose our grid and that will help CBs define specifications for the development and implementation of CBDC systems.

5. 1. Dimension 1—permissioned or permissionless

The first decision a CB has to take when it considers designing a system for a CBDC is the type of distributed ledger to use. In the DLT literature there exist two broad ledger categories for creating blockchains—permissioned and permissionless.

A permissioned ledger requires that nodes be identified and authorized before becoming transaction validators (Peters and Panayi, 2016). Permissioned ledgers are not fully decentralized because they reintroduce this form of control. The permissioned category can be further split into two subclasses, one with a single, centralized authority and one with a partially decentralized one (Buterin, 2015). A blockchain with a central authority acting as the unique validating node(s) is a special case solution. Such a system can be considered as a form of blockchain RTGS and ensures that the CB has full control over the network. There is, however, no distributed maintenance and one could argue that the CB would, in such a case, simply use advanced accounting software rather than a blockchain (Glaser, 2017).

Permissionless ledgers allow any node to participate in the validation process (Hyperledger, 2016). Strictly speaking, a permissionless ledger has no central authority (ASTRI, 2016) and the code in the fabric layer represents the ledger's rules. The fabric layer cannot be modified unless a majority of the network decides to do so, usually resulting in a fork in the blockchain. A CB could create a permissionless blockchain and leave all decisions to the majority of nodes. This is, however, highly unrealistic because a CB would most likely want to keep the fabric layer and all final decisions regarding modifications proprietary. Additionally, permissionless means that any node can start verifying transactions on the CB's blockchain. In such a case, the CB would not be able to exercise any form of control with regard to the participants and a protocol, such as PoW or PoS, would be required to secure the network. It is important to note that many authors do not distinguish between validators and users. We use a second categorization level based on the nomenclature of Peters and Panayi (2016), which defines a ledger with identified and authorized users as private, while a ledger without such control is defined as public.

Of course, a mixture between a permissioned and a permissionless blockchain can also be defined. In such a partially decentralized blockchain the CB would implement a procedure for granting transaction validating rights (making it a private blockchain) and then allow agents with rights to operate freely in the system. This hybrid approach can be open to any node or validators can be arbitrarily selected by the CB. This is illustrated by Danezis and Meiklejohn (2015) with the consortium scenario of "mintettes" presenting blocks of collected and validated transactions to the CB. The CB could, for example, designate commercial banks as validating nodes. Since all commercial banks hold an account at the CB, any fraudulent activity could be easily punished.

In permissioned or partly permissioned blockchains the CB would need to implement or delegate KYC procedures prior to any transactions taking place on the blockchain (Swanson, 2015). This blockchain's central authority would then produce a white list of authorized validators

(Hyperledger, 2016). These nodes would be identified and held legally accountable for their behavior such that the system would assume their honest behavior, which would minimize the risk of a Sibyl attack (ASTRI, 2016; Swanson, 2015). In addition, permissioned blockchains are faster and less costly to run (Pilkington, 2015).

5. 2. Dimension 2—consensus protocol

As described by Swanson (2015), "a consensus mechanism is the process in which a majority (or in some cases all) of network validators come to an agreement on the state of a ledger". Hence, a protocol is required to reach such a consensus. The type of ledger (permissioned or permissionless) has an influence on the protocol used. Permissioned blockchains can securely run on variants of Byzantine-fault-tolerance (BFT) or practical Byzantine-fault-tolerance (PBFT) protocols (Cachin, 2016), and do not require the PoW or PoS security level because they limit admission to the consensus mechanism (Monax, 2017) to nodes that are identified and held responsible for their behavior. Permissionless blockchains do not control admissions and allow dishonest nodes to join the network. This creates the risk of a "51%" or Sybil attack (Yermack, 2017). If the majority of nodes are malicious, fraudulent transactions can be validated. Eyal and Sirer (2014) show that "even a honest nodes majority [*sic*] is not always sufficient to avoid such attacks". Hence, the network is vulnerable under a standard BFT consensus (Lamport et al., 1982). PoW is the solution currently used to secure such networks. Additionally, research is being carried out into developing PoS protocols and variants, an example of this being CASPER in the Serenity version of Ethereum (Buterin, 2015).

As per Lamport, Shostak, and Pease (1982) and Tanenbaum and Van Steen (2007), BFT protocols and variants are used to reach consensus in the presence of a limited number of unresponsive or malicious nodes. Nevertheless, if nodes have nothing to lose, they might have an incentive to misbehave and validate fraudulent transactions. Permissioned blockchains

mitigate this risk by selecting honest nodes or by making punishment costlier than the returns of malicious strategies. Hence, they are resilient to nodes' erratic behavior or crashes. As their nodes cannot be punished or controlled, permissionless networks are not secured using BFT protocols.

Under the assumption that the majority of nodes are honest, the PoW protocol is "an economic incentive to mine and protect the integrity of data" (Monax, 2017). It protects permissionless networks from malicious nodes adding blocks of transactions to the blockchain. All participating nodes, colloquially referred to as miners (ASTRI, 2016), must solve a cryptographic puzzle before adding a block of validated transactions to the chain (Eyal and Sirer, 2014). This computationally intensive investment is rewarded by the right—for the successful miner(s)—to record a certain quantity of new coins in the blockchain (Yermack, 2017). Competition between miners makes fraudulent blocks and their reward likely to be disregarded. This is comparable to the punishment cost for misbehavior in permissioned blockchains. Yet PoW protocols are costly and limited in terms of their scalability. As argued by Swanson (2015), "in the long run it costs a Bitcoin to make a Bitcoin". Considering a CBDC system similar to Bitcoin, miners will increase their computational power until the potential reward is no longer profitable. Hence it will cost a CBDC unit to make a CBDC unit. Additionally, current PoW protocols limit transaction throughput but "more aggressive scaling will in the longer term will require fundamental protocol redesign" (Croman et al., 2016).

PoS-based protocols transfer decision-making power to entities holding a stake in the system (Bentov, Lee, Mizrahi, and Rosenfeld, 2014). Buterin et al. (2014) argue that PoS has numerous advantages over PoW. The idea behind PoS is to eliminate the costly computational tasks of PoW protocols while retaining the censorship resistance of permissionless blockchains. Numerous PoS concepts, including PPCoin (King and Nadal, 2012) or Proof-of-Activity (Bentov, Lee, Mizrahi, and

Rosenfeld, 2014), have been developed but do not yet ensure secure and efficient consensus (Croman, Decker, Eyal, Gencer, Juels, Kosba, Miller, Saxena, Shi, Sirer et al., 2016).

5. 3. Dimension 3—money creation: fabric layer, mining, and coloring

The third dimension in designing a CBDC system addresses the process used to generate the currency itself. As per Glaser (2017), coins can be inherent to the system or generated by a script implemented in the fabric layer. To record transactions on a blockchain, uniquely defined objects must be created. The blockchain nomenclature usually defines such objects as coins or tokens (Pilkington, 2015). We discuss a two-step decision scheme for such a process. In the first step, the CB chooses between creating coins as a reward for validating transactions (referred as a mining-like system), creating coins directly in the fabric layer (referred as a fabric-layer system), and creating coins in a hybrid scheme that encompasses both approaches (referred as a hybrid system). In the second step the CB defines the status of the coin. Pilkington (2015) defines digital coins as value-based containers and argues that coins are not strictly equivalent to currencies. Still, Danezis and Meiklejohn (2015), as well as Andolfatto (2015), consider scenarios where coins are the currency. We consider both cases: the “coin–currency” case and the “coin–container” case. In addition to these technical constraints, the generation process must take into consideration the following three criteria: First, the level of control the CB has over the monetary supply. Second, the incentives offered to validators in the system (if applicable). Third, the flexibility in terms of hosting off-chain assets.

In a mining-like system, coins can be generated as rewards for validators adding new blocks of transactions. As is the case on various permissionless networks (Nakamoto, 2008; Buterin et al., 2014), newly mined coins are distributed among successful participants in return for their computationally intensive investment. Unless fiat currency is destroyed in parallel, the CB pays

miners to run the blockchain by expanding its balance sheet without collateral. This generation process, however, is not directly applicable in permissioned networks because there is no need for PoW or PoS competition. Still, as proposed by Danezis and Meiklejohn (2015) the CB can allow a mining-like reward to authorized validators in return for their work. As there is no winner in the computational competition, the CB decides how many new coins to award and to whom these new coins belong. Hence, a clear division process is needed. In a fabric-layer system**,** coins are generated directly in the fabric layer of its blockchain, in a similar fashion to Ripple (Warren, 2017). In such a system, the CB has full control over the money supply and can add or remove coins at any time by modifying the fabric layer. In a hybrid system the CB generates a stock of coins in the fabric layer and a set of mining-like coin rewards for validators. This system offers more flexibility in terms of incentivizing validators and subsidizing transaction fees.

Irrespective of the coin generation process, a CB must define the coin either as the currency itself or as a container of the currency. The difference might seem subtle but has considerable implications for the blockchain's design. Both coins are similar in their capacity to transfer value within a system, but differ in the way they are valued.

Defining the coin as the currency itself implies that each coin in the system corresponds to one unit of the currency (assuming exchange at par). If the generation takes place in the fabric layer, the CB is in control of the digital money supply, like the current system with commercial banks. In a mining-like system, in which a deterministic number of coins is generated with each new block, the CB can control the supply of money. Better control of the supply is achieved if the reward can be arbitrarily modified by the CB. This creates, however, issues for the mining-like incentive scheme. Still, all coins given to external actors can be seen as direct payments made by the CB for running the system. Coin–currency emission implies the creation and maintenance of a new

blockchain, built from scratch or copied from an existing ledger. This creation process can only be carried out by the CB itself or by its authorized agent(s).

Defining the token as the coin–container is equivalent to loading a container with a currency or any type of asset (Rosenfeld, 2012). This minting action modifies the coin's value. "Within the notion of currency is the idea of a demurrage currency. Demurrage means carrying cost –that is, the cost to carry an asset" (Swan, 2015). Like fiat currency, the coin can be compared to the paper and ink used to print banknotes, while its face value is the currency the coin contains. The CB must choose between a fixed coin–currency value or a virtual container holding this value. A CB can hold a stock of coins and mint the currency needed without having to modify the fabric layer. Although a proprietary blockchain seems to be the most realistic solution for a CB, it is not mandatory with tokens. Several CBs can decide to run a shared blockchain and mint their CBDCs on the coins, enjoying foreign exchange transaction benefits from being recorded on a single blockchain. Additionally, other assets can be recorded on the blockchain. An interesting example is government bonds.

Mining-like reward offers greater flexibility in terms of motivating validators and subsidizing transactions costs. Since the CB must commit to a minimum reward for blocks in order to determine the incentives for validating transactions, it keeps control over the monetary supply. Coin–currency cannot host off-chain assets, while coin–container requires two steps (coin generation and tokenization) before it can be used.

5. 4. Dimension 4–incentive scheme

Although permissioned networks are less costly to run compared to permissionless ones, there is still a need to incentivize nodes to perform transaction validation. This is valid for all cases

discussed previously, except in the case where the CB is the sole validator. The incentive is limited to two forms: transactions fees and mining-like reward in new coins. Fees are direct payments from transaction initiators, while new coins can be seen as subsidies paid by the CB for the maintenance of the system. With a hybrid generation scheme the CB has levers with which to facilitate transactions. For example, an increase in the mining-like reward can fully offset transaction fees. Incentives are straightforward for cases with coin–currency. The validating node receives CBDC paid in the form of transaction fees and, if applicable, the mining-like reward paid in the form of new currency. For coin–container, the nodes are also paid in the form of transaction fees but receive untokenized coins in the case of mining-like reward. To ensure these coins have value, the CB can commit to buying them back for later minting. The total cost of transactions depends on numerous variables, but it must cover the nodes' investments in validation if the system is to be viable. Further computations regarding these costs are beyond the scope of this work.

5. 5. Dimension 5—right to transact

The CB has to decide who is entitled to hold CBDC and to carry out transactions on the network. A private blockchain implies that only identified and authorized users have the right to hold CBDC and carry out transactions. Similar to the process that the CB needs to use to decide which nodes can participate in the blockchain, this implies a KYC procedure. A straightforward solution is for the CB to delegate these procedures to commercial banks or authorized companies and let them generate wallets for the users entitled to hold CBDC. In this way, it is only possible for authorized users to hold a valid wallet. This right can be limited to certain agents in the system or be open to anyone who clears a KYC procedure.

A public blockchain is pseudonymous, as it allows anyone to hold a wallet and exchange CBDC without disclosing their identity. This is a key feature of crypto-currencies such as Bitcoin. Such a

solution seems unrealistic however in the context of CBDCs for at least two reasons: tax and AML regulations. Concerning tax, “voluntary compliance is not a workable solution since taxpayers have little incentive to report something that is not likely to be detected” (Bal, 2014). Voluntary compliance could be avoided by automatically taxing the CBDC unless ownership is declared. It is, however, a complex and costly feature to implement in the blockchain. Additionally, a public blockchain raises new difficulties with regard to the enforcement of AML regulations as “it appears unlikely that a KYC principle can be enforced in the Bitcoin system” (Moser, Bohme, and Breuker, 2013). Hence, a public blockchain is not a viable scenario for a CBDC.

5. 6. Dimension 6—awarding of money

The CB has to develop a procedure to introduce the money generated into the system. This is a two-step decision. The first step defines who has the right to transact CBDC with the CB while the second step defines the channels via which to transfer CBDC through the system. As we discuss in Section 5.5, the right to transact can be awarded only to those users who are identified and authorized following a KYC procedure.

If the CB wished to replicate the current system, it would have to consider two user classes—namely, commercial banks and all other agents that are not commercial banks. As in the current banking system, commercial banks could be licensed to hold accounts at the CB and to pledge collateral against digital currencies. Besides commercial banks, anyone who wished to use the CBDC, including all governmental bodies, financial intermediaries, companies, and citizens, would be required to obtain it through a commercial bank. Allowing direct access to the CBDC for this class has considerable KYC implications. It is not realistic for a CB to verify the identity of all users; hence, this process has to be delegated to commercial banks or authorized intermediaries. In such a case, access to the CBDC would need to pass either by a collateral channel or by a mining-like channel.

The collateral channel would be an approach similar to that currently taken with commercial banks. It implies pledging collateral to the CB in exchange for CBDC. Collateral can take many forms (Committee et al., 2013) but is often a highly liquid financial instrument, such as government bonds (European Central Bank, 2017). The collateral channel is available to both user classes. As proposed by Barrdear and Kumhof (2016), any user could pledge government bonds in exchange for CBDC.

The mining-like channel implies the existence of a reward for validating blocks. Both user classes can receive CBDC created through this channel. This depends exclusively on the right to become a validating node, defined in dimension 2. A further channel, the state benefit channel, implies the right for the state to transact CBDC with the CB. The state can then pay any kind of benefits, allowances, or tax refunds using CBDC. In this scheme, the state avoids using financial intermediaries to process payments and hence has a potential opportunity to economize in terms of costs. This channel is mainly limited to the second user class and most likely focused on national households. The concepts of “basic income” and negative income tax for citizens can be also considered as a channel (Harvey et al., 2006).

5. 7. Dimension 7—money circulation

CBDC holding and storage is a part of money circulation. Consequently, on a permissioned and private network a CB must specify storage solutions available to users. The DLT literature usually defines the electronic holder for CBDC as a “wallet” (Swan, 2015). Most current electronic currency systems require or are linked to an account held by a third party, such as a commercial bank. A disruptive feature of DLT is that users can create, control, and bear full responsibility for their wallets (Böhme, Christin, Edelman, and Moore, 2015).

Crypto-currency wallets are an option that is similar to the physical storage of notes and coins. Some users of physical fiat currency simply keep their cash in their pockets while others carry cash concealed in money belts. Most crypto-currency wallets can be downloaded for free, while others offer additional features and security—usually providing a physical device called a "hardware wallet"—for a price. In fact, wallets do not hold the crypto-currency; rather they hold the private key that generates and controls the currency's address (Hurlburt and Bojanova, 2014). Hence, users can even code their own personal wallet or record their private key on any type of support.

These wallets can be "hot" or "cold", depending on whether they provide offline or online storage of the private key. Hot wallets are kept connected to the Internet and readily available to make transactions. For example, wallet applications on mobile phones are considered hot. As they contain the user's private key they are vulnerable to thieves and hackers (Böhme, Christin, Edelman, and Moore, 2015). It is generally recommended to keep only limited amounts of currencies in hot wallets. A good analogy to hot wallets are prepaid credit cards—such cards are widely accepted, ready to make payments, and easy to top up. Still, no rational user would keep all their holdings on such a card because it can be stolen, skimmed, or hacked.

Cold wallets are kept offline to store crypto currencies. The private key they contain can be recorded on any type of support. Most are kept on an offline and securely encrypted electronic device, but users can also write their private keys on a piece of paper before deleting all digital copies. Cold wallets are protected against online attacks but are still vulnerable if the support containing the private key is stolen or destroyed (Hurlburt and Bojanova, 2014). Cold wallets are, to some extent, comparable to savings accounts.

Accounts are provided by private companies, usually offering digital and national currency exchange services. They are comparable to conventional accounts offered by commercial banks or financial intermediaries. Account providers usually set up a password but keep the user's private key secret, hence acting as a third party between the owner and their holdings. The advantages are the quick access to an exchange and trading platform, the possibility of recovering the account in the case of password loss, and—usually—insurance against hacking. On the negative side, these services generate additional costs, security mainly depends on a third party, who can be compromised, and—as most providers require identification—privacy is limited (Moore and Christin, 2013; Böhme, Christin, Edelman, and Moore, 2015). Accounts can be considered as both hot and cold as a share of crypto-currencies is kept online and ready for transactions while the remainder is stored offline for enhanced security.

As CBDC will very likely move on a permissioned and private blockchain, all transactions can be linked to specific users. A counterparty system comparable to what is currently implemented with digital money is a straightforward solution. Vendors are responsible for collecting taxes on the products and services they sell, as well as for providing receipts of transactions. This would work in a similar fashion to current digital cash payments. Additionally, transfers can be recorded in the blockchain and can be accessible to the authorities in the case of litigation. This is mandatory to ensure that the system is compliant with tax and AML regulations (Bal, 2015, 2013). A system without counterparty implies a fully digital tax and AML enforcement directly implemented in the blockchain. Such a system would be an innovation in itself and is beyond the scope of the implementation of CBDC. This solution might, therefore, become reality following further, successful development of the technology.

As the network is private, the CB can only allow transaction between wallets, and their respective keys, owned by identified and authorized users. This requires a specific wallet with a restricted number of addresses that can be linked to the user. For example, a database centralizing all authorized addresses could be updated live and verified in parallel to transaction validation. All transactions with addresses not figuring in the database would simply be rejected. Hence, it is not realistic to simply allow any type of CBDC wallet or account, with their disparate features and security levels, to be used. The CB will, rather, issue a specific guideline and authorize only compliant CBDC wallets and account providers. Users would still be able to choose between accounts from different providers, probably from commercial banks, and between personal hot or cold crypto-currency wallets. It is important to note that hot wallets are comparable to physical cash in a wallet (or to prepaid credit cards)—if the private key is lost or stolen, the user might never retrieve their CBDC. It is therefore likely that new services will be created, including insurance policies for personal CBDC.

5. 8. Dimension 8—privacy

Before processing any transfers, a CB must define who is entitled to see transaction details. Permissioned and private networks imply that all participants are identified, from users to validators. An “opaque” blockchain limits the right to consult transaction details by limiting the right to process blocks and hold a copy of the blockchain. The CB and the validating nodes have this right because they need this information to make the blockchain function. In contrast, a “transparent” blockchain identifies validators and users but leaves all transactions public, creating a privacy issue. We focus on different scenarios of opaque blockchains rather than on a radical, and unrealistic, transparency scenario. Still, without any restrictions, authorized validators can freely browse the ledger and access complete transaction details. Hence, the nodes running the blockchain are a potential threat to privacy. This calls for solutions that satisfy privacy requirements for all users

First, it is important to clarify the nomenclature used in the ledger environment; we can do this based on the work presented in Hodor's XRP Blog (2017). Privacy relates to real users' identities, accounts, and transaction details being, usually by a third party, rendered unavailable to other agents. This information must, however, be disclosed to the legal authorities for valid reasons. Pseudonymity is specific to permissionless networks. All transactions and accounts in the ledger are public but the real identities of network users remain anonymous. Anonymity ensures that real users' identities, accounts, and transaction details are nearly impossible to obtain, even for the legal authorities.

Since a CB can only accept a permissioned and private blockchain, all pseudonymous solutions are partially ruled out. Additionally, it seems obvious in terms of legal and security concerns that a CB cannot have anonymity as one of its objectives. Hence, a credible CBDC ledger should ensure a level of privacy on the network that can be removed by the authorities if needed. It is worth mentioning that some permissioned and private blockchains—Ripple, for example—are transparent (Warren, 2017). Although their privacy can be compromised (Moreno-Sanchez, Kate, Maffei, and Pecina, 2015; Moreno-Sanchez, Ruffing, and Kate, 2017), users seem to cope with this. Still, with regard to widespread CBDC adoption it can be reasonably assumed that users want to keep private their account balance, the identity of the agents with whom they transact, and the amounts transacted.

As defined by van Saberhagen (2014), there are two requirements for anonymous transactions on permissionless networks that are also applicable to privacy on permissioned and private networks: "untraceability", or the impossibility of tracing the sender of a transaction, and "unlinkability", or the impossibility of linking two transactions to the same agent. As private networks identify users, a third requirement is added to render impossible the tracking of account

balances. In an attempt to tackle the issue of privacy, we discuss here different approaches that can serve as a solution that i) ensures a certain level of privacy in order to foster adoption, but that ii) is transparent enough for the CB to intervene in the case of litigation.

A straightforward solution might be to allow validating nodes full access to the new transactions as well as to a copy of the ledger. Since validators are known and identified, they are held legally accountable for their behavior and can be monitored and, if necessary, punished. The CB might decree specific rules for private validators in order to monitor their access to transaction information and prevent them from exploiting the data. For example, a commercial bank running a node can be forced to use servers independent from their private network and to conduct regular audits under CB supervision. Since commercial banks already process and know details from numerous client transactions, this does not change much for the general public. Additionally, multiple nodes having access to data make AML enforcement easier (Bal, 2013). Still, this is not suitable for all transactions and might compromise trust in the new blockchain system because untraceability, unlinkability, and balance track are only enforced from a legal point of view rather than being a hard-coded function in the fabric layer. Hence, this solution is interesting because of its technical simplicity, but might not ensure a sufficient level of privacy for all users.

There are multiple solutions available on the technical side of blockchain to tackle privacy issues. These solutions are implemented with regard to the way transactions are carried out or are coded in the fabric layer. It is important to note that most of these methods were developed to achieve anonymity on networks. As legal authorities would not be able to obtain data should misbehavior occur, anonymity is a suboptimal result for a CBDC system. Hence, any cryptographic solution must ensure privacy but be carefully implemented to avoid anonymity. A hybrid solution, composed of code and backed by legal requirements, might be a credible solution. We detail two general methods: encryption for weak pseudonymity and secure multiparty computation.

Subsequently, we discuss potential applications of methods currently employed on blockchains, such as CoinJoin, which is used for some Bitcoin transactions (Maxwell, 2013), Monero coins, which employ ring signatures (van Saberhagen, 2014), and zero-knowledge succinct non-interactive argument of knowledge (zk-SNARK), which is one of the key features of Zerocash coins (Sasson, Chiesa, Garman, Green, Miers, Tromer, and Virza, 2014).

Encryption is the act of enciphering any type of information, commonly referred to as “plaintext”, to produce a “cyphertext” that can only be read by the holder of the respective secret encryption key (Delfs and Knebl, 2015). This form of data protection can be applied in a CBDC system, with the real identities of users being encrypted to recreate weak pseudonymity on the private network. Authorized KYC providers that are allowed to encrypt identities must keep and never use or reveal private encryption keys. In a similar fashion to traditional banking systems, these keys can only be disclosed to the legal authorities in response to valid warrants. Assuming that the KYC service market is fragmented and monitored by the CB, misbehavior and collusion between providers are both unlikely. The following example summarizes the method’s advantages. Consider Alice, who makes a purchase she would like to keep private. She can either pay in cash or use a CBDC; if she opts for a CBDC, she only discloses her encrypted identity. Even if the blockchain is transparent, the merchant sees the account but cannot identify Alice. As the transaction is directly and irrevocably settled the merchant does not need to know this information. If Alice tries to commit fraud, however, it is always possible for the authorities to identify her. This method does not enforce untraceability and unlinkability for transactions; nor does it protect against balance track, even for opaque blockchains. By inference, a prying node could identify some users. Nevertheless, it adds a layer of privacy that, in conjunction with legal requirements and additional methods, could provide sufficient protection.

Secure multiparty computation (SMPC) is defined by Zyskind, Nathan, and Pentland (2015) as "data queries that are computed in a distributed way, without a trusted third party". They continue: "Data is split between different nodes, and they compute functions together without leaking information to other nodes. Specifically, no single party ever has access to data in its entirety; instead, every party has a meaningless (i.e., seemingly random) piece of it". An informal way of describing SMPC is to think of it as a shared secret, where each node has a part of the secret that is useless if not completed by all other parts. Such a solution can be implemented for identities and transactions, ensuring, by its design, that nodes do not have access to any information. Untraceability, unlinkability, and balance track can be achieved but they need to be hard-coded in the fabric layer. Still, SMPC would require a back door to ensure that the CB and the legal authorities have access to the data. This creates a considerable risk, but one that could, however, be mitigated. As the network is permissioned and nodes are identified, it is assumed that an attack on the system is difficult to hide and is rendered extremely costly by punishment.

CoinJoin is based on the concept of joining transactions to produce one indistinguishable or atomic transaction. Its author, Maxwell (2013), states: "[w]hen you want to make a payment, find someone else who also wants to make a payment and make a joint payment together". The receiver is paid the predetermined amount by the joint transactions without knowledge of the exact sender. As each agent can only observe their own transaction in the pool, the privacy benefits of a two-transaction pool are limited. Still, an increase in the number of agents willing to join payments increases agents' privacy. Agents only observe what goes into, and out of, the pool. Hence, large pools make transaction inference less likely. Additionally, CoinJoin does not need to be coded in the fabric layer. In this context, untraceability and unlinkability are partially achieved while balance track is still possible. Given how CoinJoin is currently used on the Bitcoin network (Van Wirdum, 2016), it appears that the most efficient pool generators are dedicated servers.

Transactions details, however, are available to the agent who controls the server. This issue can be mitigated in a permissioned blockchain. Under the assumption that the number of transactions requiring a special level of privacy is limited, the CB can run these dedicated servers for an additional fee and send a pooled transaction to validators when sufficient privacy criteria are met. Additionally, as the CB maintains full knowledge of all transactions processed, the legal authorities can access the data.

Ring signatures are used to produce individual transactions signed by multiple keys. Hence, “[a] verifier is convinced that the real signer is a member of the group, but cannot exclusively identify the signer” (van Saberhagen, 2014). There are several versions of this protocol, some requiring a trusted third party while others do not. Assuming the CB can always act as a trusted third party, or closely monitor authorized agents, the first version of ring signatures can be used. This also ensures access to the data for the legal authorities. This protocol enforces untraceability and unlinkability but does not protect against balance track.

Zk-SNARK is “a proof construction where one can prove possession of certain information, e.g. a secret key, without revealing that information, and without any interaction between the prover and verifier” (Zcash, 2017). Although zk-SNARK’s functioning is nontrivial, Sasson, Chiesa, Garman, Green, Miers, Tromer, and Virza (2014) propose an intuitive example. Assume that identities behind accounts on the network are encrypted but that Alice wants to prove that she owns 100 units of the CBDC. Using her private key, she could prove she is the holder of an account containing 100 units of the CBDC, but would—in the process—disclose her whole transaction history and reveal a lot of private information. Instead, she can use a zk-SNARK to prove that she effectively owns what she claims to own, but without disclosing any other information. These powerful proofs have numerous potential applications, but it is not yet clear how they could be implemented in a CBDC system. Based on the example of ZCASH (Zcash,

2017), if hard-coded in the fabric layer, untraceability, unlinkability, and balance track can be achieved. A drawback is that they might hinder access to the data for the authorities. Hence, developments of zk-SNARK on blockchains are something that should be followed closely.

Privacy is a key feature for the future users of CBDC systems and will impact the adoption of the new currencies. A CB must ensure privacy but avoid anonymity. There are, as seen in the previous examples, as yet no perfect solutions. Still, a combination of methods can provide solutions that ensure privacy while avoiding anonymity. Encrypting identities might be sufficient for standard transactions, while sensitive transactions could use a closely monitored CoinJoin or ring signatures solution. An additional layer of legal requirements would ensure that no node has incentives to attack the privacy features of the network. This would make CBDC more private than traditional banking; not far from to the privacy offered by cash, with all the advantages of a digital currency.

5. 9. Dimension 9—scalability

Scalability is one of the most debated topics with regard to permissionless blockchains (James-Lubin, 2015). The best example is the as yet unresolved limitation to throughput on the Bitcoin network. There are two main bottlenecks in such networks: block size and block interval (Croman et al., 2016). This has two major implications. Depending on block size and interval, the number of transactions per second is bounded and the waiting time before a transaction is confirmed can be considerable. A comparison point is the VISA network, which confirms an average of 2,000 transactions per second (Croman et al., 2016). Many altcoins were developed with the objective of improving transaction throughput (McConaghy et al., 2016; Eyal, et al., 2016; Luu et al., 2016). Although scalability is a serious limitation of permissionless networks it has limited impact for permissioned blockchains. This assertion is empirically confirmed by functioning permissioned

networks such as Ripple, which supports 1,000 transactions per second with an average processing time of less than four seconds (Warren, 2017), and Hyperledger (Dinh et al.,2017). Additionally, the emission of CBDC on a permissioned network has been explored and simulated by RSCoin. The number of transactions per second and the confirmation time were not significant limiting factors (Danezis and Meiklejohn, 2015).

Hence, scalability on a permissioned blockchain is an important aspect to consider when developing the fabric layer, but it is reasonable to assume that it will not be a major obstacle.

Figure 1 represents the 9-dimensions grid that is composed by the 9 dimensions that we have discussed. Each dimension in the grid is boxed and ordered from I to IX in roman numbers. Each dimension can take different values. As an example, we can observe that the Dimension I (Permission Type) can take two values (Permissioned or Unpermissioned). The values within each dimension are also boxed. The value's box in the dimension has a background color that can be either grey or white. We consider values contained in a white box unrealistic in the current economic system or technically unfeasible, whereas we consider values contained in a grey box as realistic and feasible. Dimension VI contains a sub-dimension that states the "User Class" of the CBDC. Independently of the system chosen to award the money (Mining-like, Collateral, State benefits, or Basic Income) the user class needs to be defined by the owner of the system. As we have previously described in section 5.6. the "User Class" can be a Commercial Bank, or another entity referred in the table as "Other".

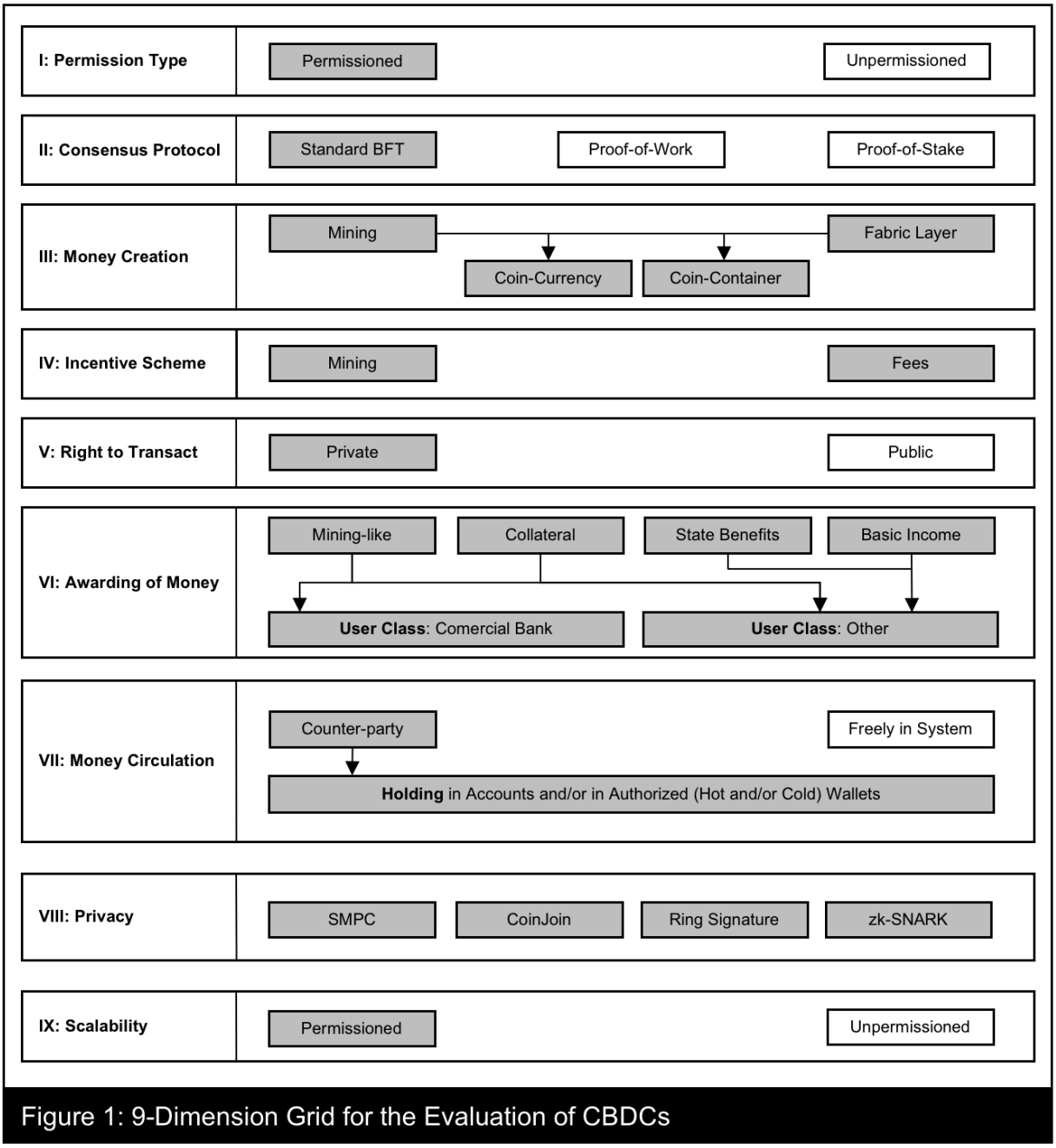

Figure 1: 9-Dimension Grid for the Evaluation of CBDCs

6 Scenario comparison

As we have shown, the choice of scenario is very broad and offers numerous possibilities. This section analyzes three out of all the possible scenarios. Scenario A proposes a smooth transition to CBDC and limits the instability that such a new system could bring with it. In terms of the current

state of blockchain technology's adoption and acceptance, Scenario A is the most probable and credible way for a CB to emit CBDC. Scenario B exploits the disruptive potential of blockchain technology by allowing end users to directly trade with the CB. Scenario C is a reflection on an international CBDC system. Table 1 summarizes the features used in each scenario.

6.1 Scenario A: electronic currency on blockchain technology

One of the primary objectives of a CB is to ensure financial stability (Padoa-Schioppa, 2003). However, blockchain technology is widely recognized for its disruptive potential with regard to the financial sector (ASTRI, 2016). Hence, it is reasonable to assume that a CB would gradually introduce a CBDC system with similar features to the current digital currency system. In this scenario, we discuss a conservative way in which commercial banks might benefit from some of the advantages of blockchain but without deviating too much from the current banking system.

Control and consensus: Based on Danezis and Meiklejohn (2015) the CB would create a permissioned blockchain in which authorized agents would be allowed to mine. These agents would be referred to as mintettes and would be exclusively formed by national commercial banks or financial intermediaries. A banking or financial license would grant the right to validate transactions on the blockchain. The BFT protocol would be used to ensure consensus among nodes. All actors would be identified in the CB's jurisdiction, such that there would be no need for PoW or PoS protocols to ensure resilience against malicious nodes.

Money creation and incentive scheme: Since implementing coin–containers would add significant complexity to this scenario, here we consider only coin–currency. Coins could be generated using both methods discussed in Section 5.3. The main generation source, however, would be the fabric layer, and the coins would belong to the CB the moment they were created. Coins generated in new blocks would only represent a small fraction of the total number of coins

available in the system because generating a large share of coins as a reward for validators would restrict CBDC emission volume. Therefore, a large source of coins would be generated by the fabric layer and a small fraction by block reward. The precise split between the two sources would need to be studied further.

Right to transact: In this system all users need to be identified and authorized before purchasing and transacting CBDC. Given their expertise, national commercial banks and financial intermediaries could be entitled to perform this authorization with regard to potential users and to award them the right to transact. CBDC accounts would work like today's bank accounts. Users could also decide to be fully responsible for their CBDC by paying for the authorization procedure and choosing a proprietary wallet.

Awarding and circulation: In this scenario, CBDC distribution would replicate the conventional scheme in which commercial banks act as intermediaries between the CB and end users. Commercial banks would have the exclusive right to pledge collateral in exchange for CBDC. Hence, a conventional bank account would be a prerequisite to purchasing CBDC. This would also add significant AML protection during the system implementation period because the "ramp-on" (buying CBDC with electronic currency) and "ramp-off" (selling CBDC) would be monitored.

Privacy: In this scenario, total privacy for users would be supported. The entities authorizing users and activating addresses would need to encrypt users' identities such that no real user would appear in the blockchain. Any attempt made by a node to identify users would be illegal and would be punished. Still, as some attributes of blockchain technology would render such behavior possible (Juhász et al., 2016), the CB would run CoinJoin servers to process sensitive transactions for an extra fee.

Scalability: As shown by Danezis and Meiklejohn (2015) and previously discussed in Section 5, scalability is not an issue for a permissioned blockchain and can be optimized by modifying the number of nodes.

This scenario proposes a realistic implementation of CBDC by leveraging the CB's network of commercial banks and limiting the potential risk of instability.

6.2. Scenario B: direct CB scheme

The disruptive potential of blockchain technology can create the conditions for a CB to trade directly with end users. This solution, however, has major implications for monetary policy and commercial banks' business.

Control and consensus: The CB would implement a permissioned blockchain in which identified, authorized agents would gather and validate transactions. At the same time, any person or entity meeting the requirements set by the CB could become a node on the network. The consensus would be reached by BFT. As we discuss with regard to Scenario A, there is no real competition; hence, the CB would need to decree a clear reward scheme for nodes participating in the system.

Money creation and incentive scheme: All the coins would be generated in the fabric layer and become the property of the CB. They would be defined as coin–currency and would be equivalent to hard or electronic currency. The reward would only be composed of transaction fees because recording new coins while adding a block would not be possible. Still, the CB could subsidize the system, during its implementation for example, by paying high fees on a few transactions in each block.

Right to transact: The blockchain would be private; hence, any user would need to be identified and authorized before accessing the network.

Awarding and circulation: CBDC would be available to all users. Based on the proposal of Barrdear and Kumhof (2016) the CB would allow anyone to directly trade government bonds in exchange for CBDC. Users would also have the opportunity to exchange hard and electronic currency for CBDC. In addition to the collateral channel, the state would gradually start to pay benefits in CBDC. The CB could decree a list of authorized wallets and account providers, with validated addresses, for users to choose from. Limited amounts could be easily exchanged online or through resellers and ATMs, in a similar fashion to current prepaid credit cards, while larger amounts would require processing by a commercial bank. Money would circulate in a classical counterparty fashion, in which vendors would need to issue receipts for transactions.

Privacy: Like in Scenario A, the blockchain would be controlled and validated at the national level and owned by the CB. Hence, first-level privacy would be ensured by pseudonymity and legal requirements for the validators. Entities authorizing users and activating addresses would need to encrypt identities. No real user name would appear in the blockchain. Any attempt made by a node to identify users would be illegal and subject to punishment. Still, as nodes would not be limited to commercial banks and financial intermediaries this would increase the risk of a privacy breach. Therefore, the CB could implement SMPC on the blockchain to divide information among nodes, making collusion less likely.

Scalability: As the number of nodes would be higher than in Scenario A, scalability is not a potential issue for such a permissioned blockchain.

6.3. Scenario C: major CB consortium

This scenario anticipates a disorganized development of CBDCs among different CBs. CBDC foreign exchange could eventually lead to compatibility issues, require intermediaries between blockchains, and generate additional costs. Additionally, features, including validation times or consensus protocols, could differ. Since blockchain technology supports multiple currencies it is possible to design a single blockchain for different CBs. Still, this implies a complex design that might be costlier to run than multiple proprietary systems. We nevertheless present this system as an example of an extreme development of CBDC and blockchain technology.

Control and consensus: In this scenario, a consortium of CBs would create a permissioned blockchain under neutral control, in a similar fashion to the BIS. Based on a collectively defined and agreed procedure, each CB would be responsible for choosing validating nodes. Nodes would be identified and held responsible for their behavior. Therefore, no PoW or PoS consensus would be required and, again, consensus would be achieved using a BFT-type algorithm (Lamport, Shostak, and Pease, 1982). In this context licensed commercial banks would become the exclusive validators. In most cases, validators would only work for a specific CB and gather its national currency transactions. Still, all CBs would have the right to choose a certain number of “omniscient” nodes who could introduce national currencies into the system. Additionally, some nodes would be given the special right to process and add foreign exchange transactions to blocks. The main advantage of such setup would be that all the transactions would stay on the same blockchain, which would simplify the system and limit costs.

Money creation and incentive scheme: The fabric layer would generate as many coins as needed and would do so at its inception. The amount of money in the system would only be modified if the consortium decided to do so. Generated coins would be distributed among CBs and defined as value containers. Hence, each CB would have to tokenize the coins received with

its national currency before introducing them into the economy. Nodes would be rewarded only in the form of transaction fees and the split would be defined by their respective CBs.

Right to transact: Due to AML requirements, network access would again be private. All users would have to be authorized and identified in order to trade their national CBDCs. Additional KYC would be required for large foreign-exchange transactions.

Awarding and circulation: The CB would not directly sell to or repurchase CBDC from end users. Instead, as currently done and proposed in Scenario A, it would deal only with commercial banks, who would be responsible for retailing the CBDC. Hence, CBDC would only be introduced or removed from the system through the commercial bank channel, but could be used for transactions directly between individuals and transactions that take place outside the traditional banking system. End users would choose between ownership of the CBDC, a digital IOU from the CB equivalent to fiat, and the ownership of a liability against a commercial bank. Hence, commercial banks would have to ensure sufficient interest to attract deposits. The use of CBDC wallets, accounts, and addresses would be left to each participating country's jurisdiction but should take the form presented in the two previous scenarios. Money would circulate in a classical counterparty fashion, in which vendors would need to issue receipts for transactions.

Privacy: Privacy could not be limited only to legal requirements. As nodes from various countries could browse the blockchain, the risk of misbehavior would be high. Therefore, the network would use a mixed solution to render transactions private. Pseudonymity would be enforced by encrypting identities. Further, each country would run and monitor several CoinJoin-like and ring signature servers to ensure both untraceability and unlinkability for sensitive transactions. Again, closely monitored foreign exchange CoinJoin-like servers would process cross-currency transactions.

Scalability: Blocks of various tokenized currencies would be added by different validating clusters; hence, consensus and block broadcast scalability would require additional design. We suggest the use of “sharding”, with a shard for each currency running in parallel (Luu, Narayanan, Zheng, Baweja, Gilbert, and Saxena, 2016).

Table 1 uses the grid to compare the three scenarios that we have discussed. It is interesting to observe that while the three scenarios significantly differ in their economic characteristics, they all share many values in each dimension, such as the permission type, the consensus protocol, the money creation in the fabric layer, the right to transact, the user class, and the scalability features. Therefore, we can see how changing only certain aspects of the blockchain, has massive implications in the resulting monetary system.

Design Question	Feature	Scenario A	Scenario B	Scenario C
Permission Type	Permissioned	✓	✓	✓
	Unpermissioned			
Consensus	BFT	✓	✓	✓
	PoW / PoS			
Money Creation	Mining	✓		
	Fabric Layer	✓	✓	✓
Coin Type	Coin-Currency	✓	✓	
	Coin-Container			✓
Incentive Scheme	Mining	✓		
	Fee	✓	✓	✓
Right to Transact	Private	✓	✓	✓
	Public			
Awarding of Money	Collateral	✓	✓	✓
	Mining-Like	✓		
	State Benefits		✓	
	Basic Income			
User Class	Commercial Banks	✓	✓	✓
	Other		✓	
Money Circulation	Counterparty	✓	✓	✓
	Freely			
Privacy	SMPC		✓	
	CoinJoin	✓		✓
	Ring Signature			
	Zk-Snark			
Scalability	Permissioned	✓	✓	✓
	Unpermissioned			

Table 1: Structured comparison of the three scenarios

7 Conclusion

The growing development of blockchain technology and digital currencies will eventually enable CBs to develop CBDC systems. Empirical work by Barrdear and Kumhof (2016) estimates that a "CBDC issuance of 30% of Gross Domestic Product (GDP) could permanently raise GDP by 3%". By establishing a system based on CBDC, CBs would have the opportunity to trade currency directly with end users, avoiding intermediaries. Individuals and companies could own their own personal wallets, in which to hold a digital IOU from the CB, directly. In this context, financing debt would be less costly for states and breaking the zero lower bound would become, to a certain extent, a realistic option for CBs. In light of these possibilities, it is realistic that CBs start to consider experimenting with CBDC-based systems. Establishing a CBDC system would, however, have massive implications for the functioning of the monetary system and CBs would need to address many technical and conceptual questions before deciding on the type of CBDC system that they would establish.

In order to facilitate the analysis that CBs would need to conduct, we propose a 9-dimension grid that addresses the technical and conceptual questions that CBs would need to answer when defining a CBDC system. The function of this grid is to provide CBs with a structured way of analyzing the different implications of moving along each of the proposed dimensions. Further, we use this 9-dimension grid as a tool with which to analyze three different scenarios. They all use blockchain technology to establish a CBDC system, but significantly differ in their implications for all the participants of the system.

Scenario A represents a conservative scenario in which commercial banks would benefit from the use of blockchain technology and would be the only agents mining a coin–currency. Further, commercial banks would be the only agents in the system with the right to pledge collateral in

return for CBDC. In such a scenario, traditional money and CBDC would coexist in parallel and users of CBDC would be identified by their banks at the point of acquiring the CBDC but would remain anonymous in terms of the transactions they conduct. This scenario would retain commercial banks' role as central agents in the system and as responsible for intermediating between the CB and citizens or companies. This scenario very much resembles the existing structure of the monetary system in many countries, but improves certain aspects of transactions and accounting, mainly to the benefit of commercial banks.

Scenario B brings with it certain innovations with regard to the conception of the monetary system. It enables the CB to trade directly with end users—which would reduce the importance of the role of commercial banks in the system as compared to the majority of systems operating today. Nevertheless, each user would need to be identified and authorized before accessing the network, which would still enable a controlled rollout of the CBDC.

Scenario C presents a system in which a global blockchain would incorporate many CBDCs and would be controlled and supported by many different CBs. A consortium of CBs would create a permissioned blockchain under neutral control but would rely on commercial banks for its management and distribution. Such a system would open the door to stronger competition between CBs, reduce transactions costs, and make possible new foreign exchange trade solutions.

While these scenarios are very different from one another, the important aspect is that they each result from the application of the same grid and can therefore be compared in a structured manner. The proposed grid serves as a tool with which to further discussions regarding the design structure of CBDCs; it may also be used as the basis of further technical and conceptual development.

8 References

Agarwal, R. and M. S. Kimball (2015): “Breaking Through the Zero Lower Bound”

Ali, R., J. Barrdear, R. Clews, and J. Southgate (2014a): “The economics of digital currencies,”

Ali, R., J. Barrdear, R. Clews, and J. Southgate (2014b): “Innovations in payment technologies and the emergence of digital currencies”

Andolfatto, D. (2015): “Fedcoin: On the Desirability of a Government Cryptocurrency,” *Web Log post*.

ASTRI (2016): “Whitepaper on Distributed Ledger Technology,” *Hong Kong Applied Science and Technology Research Institute*.

Attewell, P. (1992): “Technology diffusion and organizational learning: The case of business computing,” *Organization science*, 3, 1–19.

Bal, A. (2013): “Stateless virtual money in the tax system,” .

Bal, A. (2014): “Should Virtual Currency Be Subject to Income Tax?”
Bal, A. (2015): “How to Tax Bitcoin?” *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data*, 267.

Bank of England (2017): “RTGS Tariffs,” http://www.bankofengland.co.uk/markets/Documents/paymentsystems/rtgstariffs.pdf, accessed: 2017-08-15.

Barrdear, J. and M. Kumhof (2016): “Staff Working Paper No. 605 The macroeconomics of central bank issued digital currencies,”.

Bech, M. and K. Soramäki (2002): “Liquidity, gridlocks and bank failures in large value payment systems,” *E-Money and Payment Systems Review, Central Banking Publications*, 111–126.

Bentov, I., C. Lee, A. Mizrahi, and M. Rosenfeld (2014): “Proof of Activity: Extending Bitcoin’s Proof of Work via Proof of Stake [Extended Abstract],” *ACM SIGMETRICS Performance Evaluation Review*, 42, 34–37.

Bitcoinfees 21 (2017): “Predicting Bitcoin fees for transactions,” https://bitcoinfees.21.co/, accessed: 2017-08-15.

BitFury Group (2015): “Proof of Stake versus Proof of Work, Version 1.0,” http://bitfury.com/content/5-white-papers-research/pos-vs-pow-1.0.2.pdf, accessed: 2017-08-15.

Böhme, R., N. Christin, B. Edelman, and T. Moore (2015): “Bit-coin: Economics, technology, and governance,” *The Journal of Economic Perspectives*, 29, 213–238.

Bordo, M. D. (1993): “The Bretton Woods international monetary system: a historical overview,” in *A retrospective on the Bretton Woods system: Lessons for international monetary reform*, University of Chicago Press, 3–108.

Buterin, V. (2015): “Understanding Serenity, Part I: Abstraction,” https://blog.ethereum.org/2015/12/24/understanding-serenity-part-i-abstraction/, accessed: 2017-08-15.

Buterin, V. et al. (2014): “A next-generation smart contract and decen-tralized application platform,” *white paper*.

Cachin, C. (2016): “IBM Research - Zurich, blockchain, cryp-tography, and consensus,” https://www.zurich.ibm.com/~cca/talks/ 20161004-blockchain-techtuesday-web.pdf, accessed: 2017-08-15.

Clews, R., C. Salmon, and O. Weeken (2010): “The Bank’s money market framework,” *Bank of England Quarterly Bulletin*, 50, 292–301.

Committee, B. M. et al. (2013): “Central Bank Collateral Frameworks and Practices,” *Report by a Study Group established by the BIS Markets Committee*.

Committee on Payment and Settlement Systems (2003): *Payment and Settlement Systems in Selected Countries*, Basle: Bank for Interna-tional Settlements.

Committee on Payments and Market Infrastructures (2003): “Digital currencies,” .

Croman, K., C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, E. G. Sirer, et al. (2016): “On scal-ing decentralized blockchains,” in *International Conference on Financial Cryptography and Data Security*, Springer, 106–125.

Danezis, G. and S. Meiklejohn (2015): “Centrally banked cryptocurren-cies,” *arXiv preprint arXiv:1505.06895*.

Delfs, H. and H. Knebl (2015): *Introduction to Cryptography: Principles and Applications*, Springer.

Dinh, T. T. A., J. Wang, G. Chen, R. Liu, B. C. Ooi, and K.-L. Tan (2017): “BLOCKBENCH: A Framework for Analyzing Private blockchains,” in *Proceedings of the 2017 ACM International Conference on Management of Data*, ACM, 1085–110

European Central Bank (2011a): “The Monetary Policy of the ECB: The role of monetary policy and the benefits of price stability,” https://www.ecb.europa.eu/pub/pdf/other/monetarypolicy2011en.pdf, accessed: 2017-08-15.

European Central Bank (2011b): “The Monetary Policy of the ECB: Transmission Mech-anism of Monetary Policy,” https://www.ecb.europa.eu/pub/pdf/other/ monetarypolicy2011en.pdf, accessed: 2017-08-15.

European Central Bank (2017): “Eurosystem Collateral Data,” https://www.ecb.europa.eu/ paym/coll/charts/html/index.en.html, accessed: 2017-08-15.

Eyal, I., A. E. Gencer, E. G. Sirer, and R. Van Renesse (2016): “Bitcoin-NG: A Scalable blockchain Protocol.” in *NSDI*, 45–59.

Eyal, I. and E. G. Sirer (2014): “Majority is not enough: Bitcoin mining is vulnerable,” in *International Conference on Financial Cryptography and Data Security*, Springer, 436–454.

Federal Reserve System (2017): “Open Market Operations,” https: //www.federalreserve.gov/monetarypolicy/bst_openmarketops.htm, ac-cessed: 2017-08-15.

Fung, B. S. and H. Halaburda (2016): “Central Bank Digital Currencies: A Framework for Assessing Why and How,” .

Glaser, F. (2017): “Pervasive Decentralisation of Digital Infrastructures: A Framework for blockchain enabled System and Use Case Analysis,” in *Proceedings of the 50th Hawaii International Conference on System Sciences*.

Gregor, S., "The Nature of Theory In Information Systems", MIS Quarterly, 30(3), 2006, pp. 611–642.

Harvey, P. et al. (2006): “The relative cost of a universal basic income and a negative income tax,” *Basic Income Studies*, 1, 1–24.

Hevner, A., March, S., Park, J., and Ram, S. “Design Science in Information Systems Research,” MIS Quarterly (28:1), 2004, pp. 75-105.

Hodor’s XRP Blog (2017): “XRP, Ripple, and The Difference Between Privacy and Anonymity,” https://xrphodor.wordpress.com/2017/06/19/xrp-ripple-and-the-difference-between-privacy-and-anonymity/, accessed: 2017-08-15.

Hurlburt, G. F. and I. Bojanova (2014): “Bitcoin: Benefit or Curse?” *IT Professional*, 16, 10–15.

Hyperledger (2016): “Whitepaper,” http://www.the-blockchain.com/docs/Hyperledger%20Whitepaper.pdf, accessed: 2017-08-15.

James-Lubin, K. (2015): “O’Reilly - blockchain scalability,” https://www.oreilly.com/ideas/blockchain-scalability, accessed: 2017-08-15.

Juhász, P. L., J. Stéger, D. Kondor, and G. Vattay (2016): “A Bayesian Approach to Identify Bitcoin Users,”

King, S. and S. Nadal (2012): “Ppcoin: Peer-to-peer crypto-currency with proof-of-stake,” *self-published paper, August*, 19.

Kleine, J., M. Krautbauer, and T. Weller (2013): *Cost of Cash:Status quo and development prospects in Germany*, Steinbeis-Edition.

Kobrin, S. J. (1997): “Electronic cash and the end of national markets,” *Foreign Policy*, 65–77.

Lamport, L., R. Shostak, and M. Pease (1982): “The Byzantine gener-als problem,” *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 4, 382–401.

Lansiti, M. and K. R. Lakhani (2017): “The truth about blockchain,” *Harvard Business Review*, 95, 119–127.

Luu, L., V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena (2016): “A secure sharding protocol for open blockchains,” in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, ACM, 17–30.

March, S. T., and Smith, G. F. “Design and Natural Science Research on Information Technology,” Decision Support Systems (15), 1995, pp. 251-266.

Maxwell, G. (2013): “CoinJoin: Bitcoin privacy for the real world,” in *Post on Bitcoin Forum*.

McConaghy, T., R. Marques, A. Müller, D. De Jonghe, T. Mc-Conaghy, G. McMullen, R. Henderson, S. Bellemare, and A. Granzotto (2016): “BigchainDB: A Scalable blockchain Database,”.

McLeay, M., A. Radia, and R. Thomas (2014a): “Money creation in the modern economy,” .

McLeay, M., A. Radia, and R. Thomas (2014b): “Money in the modern economy: an introduction,” .

Monax (2017): “Permissioned blockchains,” https://monax.io/explainers/permissioned_blockchains/, accessed: 2017-08-15.

Moore, T. and N. Christin (2013): “Beware the middleman: Empirical analysis of Bitcoin-exchange risk,” in *International Conference on Finan-cial Cryptography and Data Security*, Springer, 25–33.

Moreno-Sanchez, P., A. Kate, M. Maffei, and K. Pecina (2015):

"Privacy preserving payments in credit networks," in *Network and Distributed Security Symposium*.

Moreno-Sanchez, P., T. Ruffing, and A. Kate (2017): "PathShuffle: Credit Mixing and Anonymous Payments for Ripple," *Proceedings on Privacy Enhancing Technologies*, 1, 20.

Moser, M., R. Bohme, and D. Breuker (2013): "An inquiry into money laundering tools in the Bitcoin ecosystem," in *eCrime Researchers Summit (eCRS), 2013*, IEEE, 1–14.

Nakamoto, S. (2008): "Bitcoin: A peer-to-peer electronic cash system," .

Padoa-Schioppa, T. (2003): "Central banks and financial stability: explor-ing the land in between," *The Transformation of the European Financial System*, 25, 269–310.

Peters, G. W. and E. Panayi (2016): "Understanding Modern Banking Ledgers through blockchain Technologies: Future of Transaction Process-ing and Smart Contracts on the Internet of Money," in *Banking Beyond Banks and Money*, Springer, 239–278.

Pilkington, M. (2015): "blockchain technology: principles and applica-tions," .

Rambure, D. and A. Nacamuli (2008): *Payment systems: From the salt mines to the board room*, Springer.

Research, A. B. (2016): "Understanding the cost of handling cash in Asia Pacific," *Wincor Nixdorf*.

Brown, R. (2013): "How Money Moves in Banking System," https://gendal.me/2013/11/24/a-simple- explanation-of-how-money-moves-around-the-banking-system/, accessed: 2017-08-15.

Brown, R. (2014): "Fees in the Payment Card Industry," https://gendal.me/ 2014/08/09/a-simple-explanation-of-fees-in-the-payment-card-industry/, accessed: 2017-08-15.

Rosenfeld, M. (2012): "Overview of colored coins," *White paper, bitcoil. co. il*.

Rossi, S. (2004): *Central bank money and payment finality*, Centro di studi bancari Villa Negroni-RME LAB Research Laboratory of Monetary Economics.

Sasson, E. B., A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza (2014): "Zerocash: Decentralized anony-mous payments from bitcoin," in *Security and Privacy (SP), 2014 IEEE Symposium on*, IEEE, 459–474.

Scott, S. V. and M. Zachariadis (2010): "A historical analysis of core financial services infrastructure: society for worldwide interbank financial telecommunications (SWIFT)," .

Swan, M. (2015): *blockchain: Blueprint for a new economy*, O'Reilly Media, Inc.

Swanson, T. (2015): "Consensus-as-a-service: a brief report on the emer-gence of permissioned, distributed ledger systems," *Report, available on-line, Apr*.

Tanenbaum, A. S. and M. Van Steen (2007): *Distributed systems: prin-ciples and paradigms*, Prentice-Hall.

Tennant, D. and R. Sutherland (2014): "What types of banks profit most from fees charged? A cross-country examination of bank-specific and country-level determinants," *Journal of Banking & Finance*, 49, 178–190.

U.S. Department of the Treasury (2011): "Legal Tender Sta-tus," https://www.treasury.gov/resource-center/faqs/Currency/Pages/ legal-tender.aspx, accessed: 2017-08-15. van Saberhagen, N. (2014): "CryptoNote v 2.0, 2013," .

Van Wirdum, A. (2016): "Bitcoin Magazine, CoinJoin: Com-bining Bitcoin Transactions to Obfuscate Trails and In-crease Privacy," https://bitcoinmagazine.com/articles/ coinjoin-combining-bitcoin-transactions-to-obfuscate-trails-and-increase/ privacy-1465235087/, accessed: 2017-08-15.

Warren, A. (2017): "Ripple, Ripple Consensus Ledger Can Sus-tain 1000 Transactions per Second," https://ripple.com/dev-blog/ ripple-consensus-ledger-can-sustain-1000-transactions-per-second/, accessed: 2017-08-15.

Yermack, D. (2017): "Corporate governance and blockchains," *Review of Finance*, rfw074.
Zcash (2017): "Technology: What are zk-SNARKs?" https://z.cash/technology/zksnarks.html, accessed: 2017-08-15.

Zyskind, G., O. Nathan, and A. Pentland (2015): "Enigma: Decen-tralized computation platform with guaranteed privacy,"